 TRANSMITTAL FORM	Attorney Docket No. 2473P
--	-------------------------------------

In re the application of: **Paul CRONCE et al.**

Confirmation No: **7144**

Serial No: **09/503,778**

Group Art Unit: **2134**

Filed: **February 14, 2000**

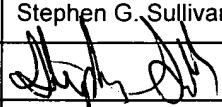
Examiner: **Ho, Thomas M.**

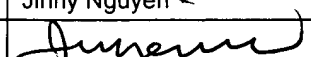
For: **Portable Authorization Device for Authorizing Use of Protected Information and Associated Method**

ENCLOSURES (check all that apply)			
<input type="checkbox"/>	Amendment/Reply	<input type="checkbox"/>	Assignment and Recordation Cover Sheet
<input type="checkbox"/>	After Final	<input type="checkbox"/>	Part B-Issue Fee Transmittal
<input type="checkbox"/>	Information disclosure statement	<input type="checkbox"/>	Letter to Draftsman
<input type="checkbox"/>	Form 1449	<input type="checkbox"/>	Drawings
<input type="checkbox"/>	(X) Copies of References	<input type="checkbox"/>	Petition
<input checked="" type="checkbox"/>	Extension of Time Request *	<input type="checkbox"/>	Fee Address Indication Form
<input type="checkbox"/>	Express Abandonment	<input type="checkbox"/>	Terminal Disclaimer
<input type="checkbox"/>	Certified Copy of Priority Doc	<input type="checkbox"/>	Power of Attorney and Revocation of Prior Powers
<input type="checkbox"/>	Response to Incomplete Appln	<input type="checkbox"/>	Change of Correspondence Address
<input type="checkbox"/>	Response to Missing Parts	*Extension of Term: Pursuant to 37 CFR 1.136, Applicant petitions the Commissioner to extend the time for response for one month(s), from August 10, 2005 to September 10, 2005.	
<input type="checkbox"/>	Executed Declaration by Inventor(s)		

CLAIMS					
FOR	Claims Remaining After Amendment	Highest # of Claims Previously Paid For	Extra Claims	RATE	FEE
Total Claims	37	45	0	\$ 50.00	\$ 0.00
Independent Claims	10	16	0	\$200.00	\$ 0.00
				Total Fees	\$ 0.00

METHOD OF PAYMENT	
<input checked="" type="checkbox"/>	Check no. 8908 in the amount of \$620.00 is enclosed for payment of appeal and extension fees.
<input type="checkbox"/>	Charge \$ _____ to Deposit Account No. _____ (Account Holder Name) for payment of fees.
<input checked="" type="checkbox"/>	Charge any additional fees or credit any overpayment to Deposit Account No. 02-2120 (Sawyer Law Group LLP).

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT	
Attorney Name	Stephen G. Sullivan, Reg. No. 38,329
Signature	
Date	August 11, 2005

CERTIFICATE OF MAILING	
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on August 11, 2005	
Type or printed name	Jinny Nguyen ~
Signature	

08/16/2005 09:00:00 00000004 03563778

120.00 OP

02 FC:1251



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

APPEAL NO:

In Re Application of: Paul A. CRONCE et al.

Confirmation No.: 7144

Serial No.: 09/503,778

Filed: February 14, 2000

For: PORTABLE AUTHORIZATION DEVICE FOR AUTHORIZING USE OF
PROTECTED INFORMATION AND ASSOCIATED METHOD

APPEAL BRIEF

08/16/2005 MAHMED1 00000004 09503778

01 FC:1402

500.00 0P

Stephen G. Sullivan
Attorney for Appellants
Sawyer Law Group, LLP
2465 E. Bayshore Road, Suite 406
Palo Alto, CA 94303

TOPICAL INDEX

I	REAL PARTY IN INTEREST	3
II	RELATED APPEALS AND INTERFERENCES	4
III	STATUS OF CLAIMS	5
IV	STATUS OF AMENDMENTS	6
V	SUMMARY OF CLAIMED SUBJECT MATTER	7
VI	GROUND OF REJECTION TO BE REVIEWED ON APPEAL	9
VII	ARGUMENTS	9
	1. Rejection under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,778,071 issued to Caputo et al. (Caputo)	9
	i) Claims 1, 2-13, and 28-35 are not anticipated by Caputo	10
	(1) Caputo fails to teach additional limitations of Independent Claims 12	13
	ii) Claims 14-15 and 36-45 are not anticipated by Caputo	14
	iii) Claims 16-19 are not anticipated by Caputo	15
	2. Rejection of claim 30 and 34 under 35 U.S.C. §103(a) as being obvious in view U.S. Patent No. 5,778,071 issued to Caputo et al.	17
IX	EVIDENCE APPENDIX	31
X	RELATED PROCEEDINGS APPENDIX	32

CERTIFICATE OF MAIL

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on August 11, 2005.


Jinny Nguyen

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

In Re Application of:

Date: August 11, 2005

Paul A. CRONCE et al.

Confirmation No: 7144

Serial No: 09/503,778

Group Art Unit: 2134

Filed: February 14, 2000

Examiner: Ho, Thomas

For: PORTABLE AUTHORIZATION DEVICE FOR AUTHORIZING USE OF
PROTECTED INFORMATION AND ASSOCIATED METHOD

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Appellant herein files an Appeal Brief drafted in accordance with the provisions of 37
C.F.R. §41.37 as follows:

I REAL PARTY IN INTEREST

Appellant respectfully submits that the above-captioned application is assigned, in its
entirety to Pace Anti-Piracy of San Jose, CA.

II RELATED APPEALS AND INTERFERENCES

Appellant states that, upon information and belief, he is not aware of any co-pending appeal or interference which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III STATUS OF CLAIMS

Application Serial No. 09/503,778 (the instant application), as originally filed, included claims 1-27. Claims 1-19 and 28-45 are presently pending. A Preliminary Amendment dated August 5, 2003 added Claims 28-45. The Preliminary Amendment crossed in the mail with an Office Action dated November 6, 2003. Consequently, newly added claims 28-45 were not examined by the Examiner. In response to the Office Action (dated November 6, 2003), Claims 1-2 and 12-14 were amended, and claims 20-27 were canceled. No claim amendments were made in a Response submitted in response to an Office Action dated April 22, 2004. Claims 1-19 and 28-45 are on appeal and all applied prospective rejections concerning Claims 1-19 and 28-45 are being appealed herein.

IV STATUS OF AMENDMENTS

Amendments submitted in response to the Final Office Action dated February 10, 2005 was not entered by the Examiner (Advisory Action dated 5/5/05), notwithstanding that the amendment merely provided corrected antecedent basis for claim 28 and attempted to cancel claims 1-27 to clarify issues on appeal.

V SUMMARY OF CLAIMED SUBJECT MATTER

The present invention provides an authorization system in which a portable security device is removably coupled to a computer system to selectively authorize the use of computer programs on the host computer. Independent claims 1, 2, 14, 16, 18, 19, 28 and 32, recite an authorization system and method in which a portable security device is removably coupled to a computer system to selectively authorize the use of one or more items of protected information, including software programs on the host computer. The portable security device receives and stores multiple items of authorization information that are associated with respective ones of the items of protected information. The portable security device includes a communication interface for communicating with multiple information authorities, such as software vendors, for downloading the authorization information to the portable security device for subsequent authorization of the vendor's software or data. The authorization information is then stored within a memory in the portable security device (See Figure 1, Specification pages 7-10; Figure 10, specification pages 29-34, for example). When a user wishes to authorize use of a protected program or data on the computer, the portable security device authorizes the host computer to use the protected program or data only if the corresponding item of authorization is stored in the device (See Figure 1, Specification page 5, lines 25-27; pages 7-10, for example).

Independent claims 14 and 36 recite an embodiment where the type of authorization information stored in the portable security device includes secret keys and key selectors for generating secret keys. Each item of authorization information (e.g., secret keys) stored in the device corresponds to a particular protected items of protected information (e.g., software programs) and is provided by the vendor of the items of protected information (e.g., vendors of the programs). When use of a protected program or data on the computer is requested, the

computer transfers the key selector corresponding to the protected program or data to the portable security device. The portable security device then internally uses the key selector to generate the corresponding secret key for validation and release of the program or data on the host computer. More specifically, when access to protected software program is attempted, software running on the host computer sends a challenge number to the portable security device. Using the secret key, the device will generate and return a response number. The correct response proves that the secret key is present in the device meaning the software (program or data) is authorized. (See FIGS. 1, 2, 5, 9, and 10, Specification page 8, line 30 through page 9, pages 12-20, pages 23-32, for example).

Independent claims 16 and 18 are directed to an embodiment where the portable authorization device stores one more items of blended authorization information that were derived from a plurality of items of authorization of information. Blending is defined in the Specification on page 18 as “data derived from the blending two or more of the dynamic key selectors 171.” The authorization device is capable of “regenerating at least one of the plurality of items of authorization information from the one or more items of blended authorization information,” and “selectively authorizes the host system to use an item of protected information based upon the at least one item of authorization information.” Independent claim 19 includes similar recitation, but uses the terms “decoding information”, rather than blended authorization of information, and “decodes”, rather than “regenerating” (See, Specification page 18, line 30 - page 19, line 13; page 26, line 30 - page 27, line 6; page 27, line 31 - page 28, line 2; page 35, line 22 - page 38, for example).

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-19, 28-29, 31-33, 35-45 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,778,071 issued to Caputo et al. (Caputo).

Claims 30 and 34 stand rejected under 35 U.S.C. §103 as being obvious in view of Caputo.

VII ARGUMENTS

1. Rejection of 1-19, 28-29, 31-33, 35-45 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,778,071 issued to Caputo et al. (Caputo)

Anticipation requires that a prior art reference disclose each and every claim element of the claimed invention. It is respectfully submitted that Caputo fails to teach or suggest each and every element of independent claims 1, 2, 14, 16, 18, 19, 28 and 32.

In contrast to the present invention, Caputo is directed to a portable security device having a network communication interface that provides encryption and authentication capabilities to protect data and restrict access to authorized users (col. 1, lines 10-15). The device integrates security and interface functions to be used as an access control means to another computer or network (col. 3, lines 39-43). The portable device can be used as an identifying token, a communications network interface, a data encryptor, a user, and device and/or message authenticator. It provides an electronic token which can be carried by the user to quickly identify him or her to a network, to a computer system, or to an application program. The device contains a modem for connecting the device to a data transfer path, such as a telephone network (column 5, lines 7-15). The device will not permit communications to proceed until the device and optionally, the user, have been identified by the authenticator.

In operation, the device is connected to a network and waits for a challenge from the network or other security device. When the challenge is received, the device may prompt a user to enter a PIN. The PIN is then encrypted and the encrypted result is returned to the challenger on the network to be checked. If verification by the challenger on the network is not successful, then the challenger ends the communication session. If it is successful, then an acknowledgment is returned to the device and communications are enabled by the challenger so the network or computer is accessible (Col. 17, lines 30-56).

i) Claims 1, 2-13, and 28-35 are not anticipated by Caputo

Independent claims 1, 2, 12, 28 and 32, which are similar in scope, include recitations for a portable authorization device removably coupled to a host computer system that meets the following limitations:

- 1) stores multiple items of authorization information in memory,
- 2) each of the multiple items of authorization information are associated with a respective item of protected information that is used by a host system,
- 3) the portable authorization device is capable of receiving multiple items of information while being coupled to the host system (e.g., receiving updates or new authorization information), and
- 4) the portable authorization device must be capable of selectively authorizing the computer system to use one of the items of protected information based upon the corresponding item of authorization information being stored in the memory.

Caputo fails to teach or suggest several limitations of independent claims 1, 2, 12, 28 and 32.

First, Caputo fails to teach or suggest a portable authorization device “for selectively authorizing the computer system to use multiple items of protected information (e.g., software)” as recited in the preamble of claims 1, 2, 28 and 32. Instead, Caputo’s device verifies the identity of a user on a network, not which item of protected information to which the user has access on the host computer. If servers on a network in Caputo can verify the single identity of the device and/or the user, then access is granted. Caputo’s device does not have the intelligence to determine what multiple pieces of information on the computer the user is allowed to access or not. In Caputo, user access is ultimately controlled by the servers on the computer network, not by an external device coupled to the host computer.

Further, Caputo fails to teach or suggest a portable authorization device for selectively authorizing the computer system to use multiple items of protected information “based upon the corresponding item of authorization information being stored” in the storage medium, as recited in claims 1, 2, 12, 28 and 32. The Examiner considers challenges and user PINs disclosed by Caputo to be analogous to the multiple items of protected information. Although Appellant disagrees with this contention, even assuming arguendo that Caputo’s challenges and PINS are analogous to the multiple items of protected information, Caputo’s challenges and PINs are not stored within Caputo’s security device, and Caputo’s challenges and PINs function to allow user to access the network from the host computer, rather than to allow the host computer to which the device is connected to use items of protected information.

Caputo further fails to teach or suggest that “first” and “second” “items of authorization information” are associated with “first” and “second” “items of protected information” on the computer to which the device is connected (claims 1 and 2), or recited differently, that multiple items of authorization information “are associated with respective ones of the multiple items of

protected information” (claims 28 and 32). For example, authorization #1 must be present in the device in order to gain access to information item #1 on the computer; authorization #2 must be present in the device in order to gain access to information item #2; etc. The device can hold many of these authorizations to allow access of many items of information. Caputo fails to teach or suggest a device that meets this functionality.

The Examiner considers challenges and user PINs disclosed by Caputo to be analogous to the multiple items of protected information. Challenges are sent from a computer on a network to Caputo's device, and in response, the device prompts a user for a PIN or a smart card insertion. Challenges have nothing whatsoever to do with items of information that are associated with respective items of protected information, such as programs and data, on the computer to which computer's device is connected. Likewise, a PIN entered by the user or read from a smart card is associated with a user, not items of protected information on the computer. The PIN is merely a mechanism to prevent unauthorized use of the device, so that, for example, a thief could not use the device. The PIN adds extra security strength to proving the *identity* of the user using the device. Challenges and PIN are just used to prove identity.

In the claims of the present invention, the identity of the device or the identity of its user in no way plays a role in determining access to pieces of information, as in Caputo. In addition, a server and/or a network are not needed for the device of the present invention to grant access to the computer to use the protected information, as in Caputo.

Caputo further fails to teach or suggest that the "item of authorization information" that is associated with a corresponding "item of protected information" on the host computer is, in fact, "provided by a vendor" of the "item of protected information," as recited in independent claims 1, 2 and 12. That is, in the present invention, a vendor, of a software program, for example,

provides an item of authorization, such as a key, for storage in the portable authorization device. Then, users who have purchased the software program must then insert the portable authorization device into their computer so that the portable authorization device can use the key to unlock the software program. As described above, in Caputo, the user enters a PIN into the security device (or the PIN is read from a smart card) to gain access to network devices. This PIN, however, is not provided by the vendors of the network devices, nor is it stored in the security device. Caputo's challenges are sent from a computer over a network to the device to which the security devices attached, but are not stored in the security device, nor are the challenges associated with specific items of authorization (e.g., programs).

(1) Caputo fails to teach additional limitations of Independent Claims 12

Caputo fails to teach or suggest "an access control mechanism associated with the host system for receiving a first item of authorization information from a first type of information authority operatively coupled to the host system and for forwarding the item of authorization information to the portable authorization device," as recited in claim 12. In this embodiment, the host system receives the item of authorization information and forwards the item of authorization information to the portable authorization device for storage. This allows new items of authorization information to be downloaded into the portable authorization device from the Internet, for example. As described above, in Caputo, challenges are received over the network by the host system, but the challenges are not stored in the security device. Nor are the challenges used to authorize the host system to access protected items of information, such as software, that may be stored on the host system.

As Caputo fails to teach or suggest the elements of claims independent claims 1, 2, 12, 28, and 32, independent claims 1, 2, 12, 28, and 32 are patentable over Caputo. The arguments made above apply with full force and effect to dependent claims 3-11, 13, 29-31, and 33-35 because dependent claims incorporate the limitations of the independent claims.

ii) Claims 14-15 and 36-45 are not anticipated by Caputo

Independent claims 14 and 36 recite a portable authorization device that stores multiple key selectors, one for each item of protected information on the computer to which it is connected. When the portable authorization device receives an authorization request from the computer system to authorize use of a particular one of the items up to confirmation, the stored key selector corresponding to the particular one of the items and a shared secret are used to generate authorizing information. Once the computer system validates the authorizing information, the particular one of the items of protected information is released for use by the computer system. In addition, the key selectors are downloaded and stored in the portable authorization device prior to use.

Independent claims 14 and 36 stand rejected under §102(b), despite the fact that the Examiner rejected dependent claims 30 and 34, which include similar subject matter, under §103, explicitly admitting that “Caputo fails to explicitly disclose a method wherein a key is generated within the portable security device based upon the key selectors” (Final Office Action, pg. 22). In light of this admission, Appellant respectfully submits that the Examiner’s rejections of independent claims 14 and 36 is in error and should be reversed.

As described above, Caputo fails to teach or suggest “a portable authorization device for selectively authorizing a host system to use one more items of protected information,” as recited

in independent claims 14 and 36. In addition, it is not believed that Caputo's challenges or PINS can be considered analogous to key selectors for several reasons. First, Caputo fails to teach or suggest storing challenges or PINS in the security device, as explained above. Therefore, Caputo cannot teach storing "one key selector for each item of protected information" in the device. Second, neither Caputo's challenges nor PINs are used to "generate" a key (claim 14) or "authorization information" (claim 36) within the device based on stored the key selector, where the key or authorization information is then used to selectively authorize the host system to use the items of protected information (claim 14) or to release the item of protected information (claim 36).

Caputo may teach cryptographic keys for encryption, where the encryption could be any calculated from the decryption key and vice versa to keep the key secret (col. 11, lines 17-38). However, these are standard encryption keys used for encrypting and decrypting data transmitted over the network. Any key used to generate another encryption/decryption key would be used only for that purpose, not for validation by the computer system to release the item of protected information that key selector is associated with.

Accordingly, the reasons set forth above, it is respectfully submitted that Caputo fails to teach or suggest the recitations of independent claims 14 and 36. The arguments made above apply with full force and effect to dependent claims 15 and 36-45 because dependent claims incorporate the limitations of the independent claims.

iii) Claims 16-19 are not anticipated by Caputo

Independent claims 16 and 18 are directed to a portable authorization device that stores a "one more items of blended authorization information" "in a storage medium" that were "derived

from a plurality of items of authorization of information”. The authorization device is capable of “regenerating at least one of the plurality of items of authorization information from the one or more items of blended authorization information,” and “selectively authorizes the host system to use an item of protected information based upon the at least one item of authorization information.” Independent claim 19 includes similar recitation, but uses the terms “decoding information”, rather than blended authorization of information, and “decodes”, rather than “regenerating.”

It is respectfully submitted that Caputo fails to teach or suggest any of these limitations in claims 16, 18, and 19. The Examiner considers authorization information that is encrypted or decrypted in where a private key is “regenerated” when needed in the authorization processed be analogous to blended and unblended information. However, blending is defined in the Specification (page 18, lines 3 through page 19, line13) as “data derived from the blending two or more of the dynamic key selectors 171. The dynamic key selectors 171 are blended in a systematic way such that the dynamic key selector data 156 cannot be partitioned into segments exclusively associated with individual dynamic key selectors.” Caputo fails to teach suggest that any authorization of mission within the security device is derived from blending two or more items of authorization of information. And even if Caputo’s encrypted private keys can be considered analogous to blended authorization information, the authorization information regenerated from the blended authorization information would not be used to selectively authorize the host system to use an item of protected information based upon the at least one item of authorization information,” as recited in claims, 16, 18, and 19.

Accordingly, the reasons set forth above, it is respectfully submitted that Caputo fails to teach or suggest the recitations of independent claims 16-19.

For the reasons set forth above, it is respectfully submitted that the section 102(b) rejection of claims 1-19, 28-29, 31-33, 35-45 based on Caputo has been overcome.

2. Rejection of claim 30 and 34 under 35 U.S.C. §103(a) as being obvious in view U.S. Patent No. 5,778,071 issued to Caputo et al.

In the rejection of claims 30 and 34, the Examiner admits that "Caputo fails to explicitly disclose a method wherein a key is generated within the portable security device based upon the key selectors." The Examiner takes official notice that generating a key in either side of an authentication scheme was well-known at the time of the invention. The Examiner stated that "it would have been obvious to one of ordinary skill in the art of time the invention to generate the key inside of the portable device in order to avoid transmitting the key over an insecure line and leave the possibility open for the private key becoming compromised."

Even assuming that the Examiner is correct in his assumption, the Examiner failed to cite or state any argument to teach or suggest the generation of a key within the portable security device is "based upon key selectors" that are received by the portable security device from the host system for the purpose of authorizing the host system to use items of protected information, such as programs, (combination of claims 28-30 and claims 32-34). In an absence of any teaching or suggestion to the contrary, it is believed that claims 30 and 34 are patentable over Caputo and the Examiner's Official Notice.

Accordingly, Appellant respectfully requests withdrawal of the rejection under 35 U.S.C. 102(b) and 103(a) and respectfully requests that the Board reverse the final rejection of Claims 1-19 and 28-45.

For all the foregoing reasons, it is respectfully submitted that Claims 11-19 and 28-45 (all the Claims presently in the application) are patentable. Thus, Appellant respectfully requests that the Board reverse the rejection of all the appealed Claims and find each of these Claims allowable.

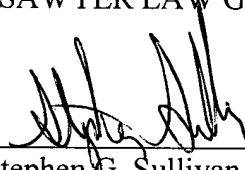
Note: For convenience of detachment without disturbing the integrity of the remainder of pages of this Appeal Brief, Appellant's "APPENDIX" sections are contained on separate sheets following the signatory portion of this Appeal Brief.

Authorization for payment of the required Brief fee is contained in the cover letter for this Brief. Please charge any fee that may be necessary for the continued pendency of this application to Deposit Account No. 02-2120 (Sawyer Law Group LLP).

Respectfully submitted,
SAWYER LAW GROUP LLP

August 11, 2005

Date



Stephen G. Sullivan
Attorney for Appellant(s)
Reg. No. 38,329
(650) 493-4540

VIII CLAIMS APPENDIX

1. (Previously Amended) A method for operating a portable authorization device for selectively authorizing a host system to use one or more items of protected information, including software, comprising:

coupling the portable authorization device to the host system;

receiving a first item of authorization information from a first type of information authority, the first item of authorization information being associated with a first one of the items of protected information and provided by a vendor of the first one of the items of protected information;

receiving a second item of authorization information from a second type of information authority, the second item of authorization information being associated with a second one of the items of protected information and provided by a vendor of the second one of the items of protected information; and

selectively authorizing the host system to use the one or more items of protected information based upon the first or second items of authorization information being stored therein.

2. (Previously Amended) A portable authorization device for selectively authorizing a host system to use one or more items of protected information, including software, comprising:

a processing unit;

a storage medium operatively coupled to the processing unit;

a first interface operative in conjunction with the processing unit and the storage medium for receiving a first item of authorization information from a first type of information authority the first item of authorization information being associated with a first one of the items of protected information and provided by a vendor of the first one of the items of protected information;

a second interface operative in conjunction with the processing unit and the storage medium for receiving a second item of authorization information from a second type of information authority the second item of authorization information being associated with a second one of the items of protected information and provided by a vendor of the second one of the items of protected information; and

a third interface operative in conjunction with the processing unit and the storage medium for communicating with the host system to selectively authorize the host system to use the one or more items of protected information based upon the first or second items of authorization information being stored therein;

wherein the portable authorization device is removably couplable to the host system through the third interface.

3. (Original) The portable authorization device of claim 2, wherein:
 - the first interface comprises a direct information authority interface program;
 - the first type of information authority comprises a direct information authority operatively coupled directly to the portable authorization device;
 - the second and third interfaces each comprise a same host system interface program; and

the second type of information authority comprises an indirect information authority operatively coupled to the portable authorization device through the host system.

4. (Original) The portable authorization device of claim 3, wherein the indirect information authority comprises a computer system coupled to the host system via a network.

5. (Original) The portable authorization device of claim 3, wherein the indirect information authority comprises data stored on a magnetic storage medium.

6. (Original) The portable authorization device of claim 2, further comprising:
a host authorizer operative in conjunction with the processing unit and the third interface for selectively authorizing the host system to use the one or more items of protected information based upon the first or second items of authorization information.

7. (Original) The portable authorization device of claim 6, wherein the host authorizer is a software program operatively stored in the storage unit.

8. (Original) The portable authorization device of claim 6, wherein:
the first and second items of authorization information comprise first and second key selectors, respectively; and

the host authorizer in conjunction with the processing unit and the third interface operatively generates a key based upon the first or second key selectors and selectively authorizes the host system to use the one or more items of protected information based upon the key.

9. (Original) The portable authorization device of claim 2, wherein the first interface is configured to conduct a challenge-response transaction with the first type of information authority.

10. (Original) The portable authorization device of claim 2, wherein the second interface is configured to conduct a challenge-response transaction with the second type of information authority.

11. (Original) The portable authorization device of claim 2, wherein the third interface is configured to conduct a challenge-response transaction with the host system.

12. (Previously Amended) An authorization system for selectively authorizing a host system to use one or more items of protected information, including software, comprising:

an access control mechanism associated with the host system for receiving a first item of authorization information from a first type of information authority operatively coupled to the host system and for forwarding the item of authorization information to the portable authorization device, the first item of authorization information being associated with a first one of the items of protected information and provided by a vendor of the first one of the items of protected information; and

a portable authorization device removably couplable to the host system for receiving the first item of authorization information from the access control mechanism and for selectively authorizing the host system to use the one or more items of protected information based upon the first item of authorization information being stored therein.

13. (Previously Amended) The authorization system of claim 12, wherein:

the portable authorization device is configured to also receive a second item of authorization information from a second type of information authority operatively coupled to the portable authorization device, the second item of authorization information being associated with a second one of the items of protected information and provided by a vendor of the second one of the items of protected information, and, furthermore, is configured to selectively authorize the host system to use the one or more items of protected information based upon the first or second items of authorization information being stored therein.

14. (Previously Amended) A portable authorization device for selectively authorizing a host system to use one or more items of protected information, comprising:

a processing unit;

a storage medium operatively coupled to the processing unit;

a first interface operative in conjunction with the processing unit and the storage medium for receiving a key selector from an information authority the key selector being associated with a first one of the items of protected information and provided by a vendor of the first one of the items of protected information;

a host authorizer operative in conjunction with the processing unit and the storage medium for generating a key based upon the key selector; and

a second interface operative in conjunction with the processing unit and the storage medium for communicating with the host system to selectively authorize the host system to use the one or more items of protected information based upon the key;

wherein the portable authorization device is removably couplable to the host system through the second interface.

15. (Original) The portable authorization device of claim 14, wherein:

the first interface comprises an information authority interface; and

the second interface comprises a host system interface.

16. (Original) A portable authorization device for selectively authorizing a host

system to use a plurality of items of protected information, comprising:

a processing unit;

a storage medium operatively coupled to the processing unit for storing one or more items of blended authorization information, each item of blended authorization information being derived from a plurality of items of authorization information;

an unblending mechanism operative in conjunction with the processing unit and the storage medium for regenerating at least one of the plurality of items of authorization information from the one or more items of blended authorization information; and

a host system interface operative in conjunction with the processing unit and the storage medium for communicating with the host system to selectively authorize the host system to use an item of protected information based upon the at least one item of authorization information;

wherein the portable authorization device is removably couplable to the host system through the host system interface.

17. (Original) The portable authorization device of claim 16, wherein:

each item of blended authorization information is derived from the two or more items of authorization information by performing an arithmetic operation on the two or more items of authorization information.

18. (Original) A method for operating a portable authorization device for selectively authorizing a host system to use one or more items of protected information, comprising the steps of:

coupling the portable authorization device to the host system;
receiving a plurality of items of authorization information;
generating one or more items of blended authorization information from the plurality of items of authorization information;
storing the one or more items of blended authorization information in a storage medium;
retrieving one or more of the items of blended authorization information from the storage medium;
regenerating at least one of the plurality of items of authorization information from the one or more items of blended authorization information; and

selectively authorizing the host system to use an item of protected information based upon the at least one item of authorization information.

19. (Original) A portable authorization device for selectively authorizing a host system to use one or more items of protected information, comprising:

a processing unit;

a first storage medium operatively coupled to the processing unit for storing one or more encoded items of authorization information;

a second storage medium operatively coupled to the processing unit for storing decoding information used to decode the one or more encoded items of authorization information, wherein the second storage medium is accessible by the processing unit only if the processing unit receives proper authorization;

a decoding mechanism operative in conjunction with the processing unit and the first and second storage media for decoding at least one of the one or more encoded items of authorization information to produce at least one respective item of authorization information; and

an interface operative in conjunction with the processing unit for communicating with the host system to selectively authorize the host system to use an item of protected information based upon the at least one item of authorization information.

20. – 27 (Canceled).

28. (Previously Presented) A portable security device removably coupled to a computer

system for selectively authorizing the computer system to use multiple items of protected information, comprising:

a processing unit;

at least one storage medium coupled to the processing unit;

an interface capable of receiving multiple items of authorization information that are associated with respective ones of the multiple items of protected information, wherein the multiple items of authorization information are stored within the at least one memory; and

an interface program for selectively authorizing the computer system to use one of the items of protected information based upon the corresponding item of authorization information being stored in the memory.

29. (Previously Presented) The method of claim 28 wherein the multiple items of authorization information comprise key selectors.

30. (Previously Presented) The method of claim 29 a key is generated within the portable security device based upon the key selectors and selective authorization is given to the computer system to use the multiple items of protected information based upon the key.

31. (Previously Presented) The method of claim 28 wherein the multiple items of authorization information comprise one or more secret keys.

32. (Previously Presented) The method for selectively authorizing the use of multiple items of protected information on a computer system using a portable security device that is removably coupled to the computer system, the method comprising the steps of:

- (a) providing the portable security device with the capability of receiving multiple items of authorization information that are associated with respective ones of the multiple items of protected information, wherein the multiple items of authorization information are stored within a single memory in the portable security device; and
- (b) selectively authorizing the computer system to use one of the items of protected information based upon the corresponding item of authorization information being stored in the memory.

33. (Previously Presented) The method of claim 32 wherein the multiple items of authorization information comprise key selectors.

34. (Previously Presented) The method of claim 33 further including the step of: generating a key within the portable security device based upon the key selectors and selectively authorizing the computer system to use the multiple items of protected information based upon the key.

35. (Previously Presented) The method of claim 32 wherein the multiple items of authorization information comprise one or more secret keys.

36. (Previously Presented) A method for selectively authorizing the use of multiple items of protected information on a computer system, the method comprising the steps of:

- (a) providing a portable security device with at least one memory containing a shared secret and space for multiple key selectors, one key selector for each item of protected information, and at least one I/O port, whereby the key selectors can be downloaded into the security device, and communications can be established with the computer system;
- (b) receiving by the portable security device an authorization request from the computer system to authorize use of a particular one of the items of protected information; and
- (c) using the stored key selector corresponding to the particular one of the items and the shared secret to generate authorizing information, wherein the computer system validates the authorizing information and releases the particular one of the items of protected information for use.

37. (Previously Presented) The method of claim 36 further including the step of providing the key selectors to the portable security device memory using external information authorities within a secure transaction.

38. (Previously Presented) The method of claim 37 further including the step of receiving a random challenge from the information authority, using the shared secret to encrypt the response, and validating by the information authority the response by decrypting with the shared secret.

39. (Previously Presented) The method of claim 36 where the shared secret is an encryption key.

40. (Previously Presented) The method of claim 39 further including the step of transforming the received key selector into an authorizing key using the shared secret key.

41. (Previously Presented) The method of claim 40 where the authorization request is a randomly generated challenge number.

42. (Previously Presented) The method of claim 41 where the authorization information is generated by using the challenge and the authorizing key.

43. (Previously Presented) The method of claim 36 further including the step of encrypting the key selectors before storing in the portable security device memory.

44. (Previously Presented) The method of claim 43 further including the step of storing the key selectors in a merged pool in memory using a blending algorithm, whereby an individual key selector cannot be extracted from a specific location in memory.

45. (Previously Presented) The method of claim 36 further including the step of receiving the multiple items of information from multiple information authorities.

IX EVIDENCE APPENDIX

(None)

X RELATED PROCEEDINGS APPENDIX

(None)